swissinfo.ch
International Service of the Swiss Broadcasting Corporation

FORSCHUNG

Papierloses, sicheres E-Voting – ein Langzeit-Projekt

Von Andreas Keiser, swissinfo.ch
Biel

09. Oktober 2013 - 11:00

Sicherheitslücken haben das E-Voting in die Kritik gebracht. Vollelektronische und sichere Systeme sind technisch zwar machbar, aber ihre Umsetzung ist anspruchsvoll und liegt in weiter Ferne. Der nächste Schritt geht nicht ohne Papier. Eine Bestandesaufnahme aus Sicht der Wissenschaft.

"Die in der Schweiz aktuell angewendeten Systeme erlauben es dem Wähler in keiner Art und Weise zu überprüfen, was mit seiner Stimme passiert ist. Er hat keine andere Wahl, als dem System zu vertrauen", sagt Rolf Haenni, Informatik-Professor am "Research Institute for Security in the Information Society" (RISIS) der Berner Fachhochschule in Biel.

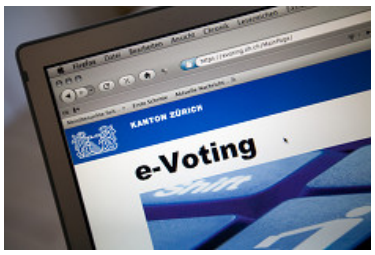
"Man hat grossen Wert gelegt auf gewisse Facetten der Sicherheit, doch den Systemen der ersten Generation fehlt eine Eigenschaft, die wir seit Jahren fordern; die Verifizierbarkeit, also die Möglichkeit für den Wähler zu überprüfen, ob seine Stimme wirklich in seinem Sinn angekommen ist", sagt Haenni's Kollege, der Direktor des RISIS, Eric Dubuis.

E-VOTING

Die direkte Demokratie im digitalen Zeitalter

Die Schweizer Regierung will dereinst die elektronische Stimmabgabe einführen. Die Umstellung auf ein globales E-Voting erfolgt aus Sicherheitsgründen aber nur schrittweise. Vorrang bei der Einführung hat die Fünfte Schweiz. [...]

Politik Auslandschweizer Direkte Demokratie



Wenn das "Ja" ein "Nein" ist

Stark vereinfacht besteht das E-Voting-System aus einem Zentralrechner, der die Stimmen auswertet und den Computern der Wählerinnen und Wähler.

Theoretisch kann ein Wahlresultat mit einem Hackerangriff auf den Zentralrechner oder mit einer Infizierung durch Malware auf den Computern der Wähler verfälscht werden. Malware kann dazu führen, dass der Wähler ohne etwas zu merken oder zu ahnen auf dem Bildschirm ein "Ja" eingibt, beim Zentralrechner jedoch ein "Nein" eintrifft.

Bei Wahlen und Abstimmungen geht es meist um handfeste Interessen. Eine Interessengruppe könnte Tausende von ungeschützten Computern infizieren und so ein Abstimmungsergebnis verfälschen. Vor einem solchen Szenario warnt die Wissenschaft seit mehr als zehn Jahren.

Die einfache Lösung, die darin bestünde, dass der Zentralrechner jedem Wähler ähnlich einer Bestellbestätigung eine Bestätigung seiner abgegebenen Stimme senden würde, kommt nicht in Frage, denn: "Das Stimmgeheimnis muss gewährt bleiben. Das System darf nicht erfahren, wie ich stimme, auch der Systemadministrator nicht. Das macht es viel schwieriger", so Haenni.

Bundesrat hält am Plan fest

Eine grosse Mehrheit der Auslandschweizerinnen und Auslandschweizer soll bei den Eidgenössischen Wahlen 2015 über das Internet abstimmen können. Der Bund hält trotz Kritik an diesem Ziel fest.

Die Diskussionen über Sicherheitslücken wurden im Juli ausgelöst, nachdem ein vom Kanton engagierter Hacker eine Sicherheitslücke im Genfer E-Voting-System offengelegt hatte.

Schwachstellen dieser Art sind den Behörden schon lange bekannt. Entsprechend der Maxime "Sicherheit vor Tempo" darf deswegen nur ein Bruchteil der Stimmberechtigten per Internet abstimmen.

Derzeit liegt die vom Bund festgelegte Limite bei gesamtschweizerisch 10%; in keinem Kanton dürfen mehr als 30% der Stimmberechtigten über Internet abstimmen. Effektiv ist E-Voting heute aber erst für rund 3% der Stimmberechtigten möglich, hauptsächlich für Auslandschweizer.

Für vier junge Nationalräte aus verschiedenen Parteien genügt diese Sicherheit indes nicht. Sie kündigten kürzlich an, sie wollten per Vorstoss das E-Voting-Projekt stoppen, mindestens bis sicherere Programme existieren. Ähnliche Vorstösse gibt es auch in mehreren Kantonen.

Nach Bekanntwerden der Probleme mit dem Genfer System klinkten sich die Kantone Uri und Obwalden aus dem Projekt aus und verzichten vorerst auf E-Voting.

Nebst dem kritisierten Genfer System, das auch Bern, Luzern und Basel-Stadt nutzen, existiert auch ein Programm aus Zürich, das acht Kantone nutzen. Über ein eigenes System verfügt Neuenburg.

In die richtige Richtung

Voraussichtlich 2014 wird in der Schweiz schrittweise die zweite Generation E-Voting eingeführt. Neu werden die Stimmberechtigten zusammen mit dem Stimmmaterial je einen individuellen, vierstelligen Code für ein "Nein" und für ein "Ja" erhalten.

Nachdem der Wähler abgestimmt hat, sendet ihm das System einen so genannten Verifikations-Code zurück. Diesen kann man mit dem Code auf dem Stimmmaterial vergleichen. Eine allfällige Manipulation würde sofort auffallen.

"Das Schiff geht nun in die richtige Richtung", sagt Dubuis, "denn weil es die Leute merken würden, ist es auch nicht mehr interessant, eine Malware zu verbreiten. Das ist ein riesiger Unterschied zum heutigen System, denn da besteht das Risiko, dass man eine Manipulation nicht bemerkt".

Transparente Urnen

Auch bei diesem System bleibt der Aufwand für die zentrale Datensicherheit und das korrekte Auszählen der Stimmen hoch. Fehler können nicht ganz ausgeschlossen werden, Manipulationen, etwa beim Druck der Codes, sind theoretisch nicht ausgeschlossen. Dubuis und Haenni plädieren deshalb zusätzlich für einen Systemwechsel, das heisst für eine "Offenlegung der Daten, insbesondere der verschlüsselten Stimmen".

Bleibt das Problem der möglichen Rückverfolgung der Daten hin zum Absender, also der Aushebelung des Stimmgeheimnisses. Die Lösung orientiert sich an den transparenten Urnen, wie sie in Frankreich gebräuchlich sind. "Man sieht, dass sie am Anfang leer sind, dann werden sie geschüttelt und keiner kann mehr erkennen, wer wie gestimmt hat", sagt Dubuis.

Pilot in Norwegen

In der elektronischen Welt heisst das: Offenlegung der verschlüsselten Daten und Anonymisierung der Daten vor dem Entschlüsseln. "Die Daten werden mehrmals kryptografisch gemixt. Die gemixten Stimmen lassen sich äusserlich nicht mehr mit den eingegangenen Stimmen in Verbindung bringen, inhaltlich aber sind sie identisch. Und dies lässt sich mathematisch beweisen", sagt Haenni.

"Das sind wissenschaftlich zertifizierte und als gültig und 100 Prozent zuverlässig anerkannte Verfahren. Und das Stimmgeheimnis wird geschützt."

Ein solches Mixsystem sei "hoch kompliziert", räumt Haenni ein. "Für die Wahlen in die Studentenräte haben wir solche Systeme eingesetzt. Wir arbeiten daran. Es gibt keine pfannenfertige Lösung, die man einkaufen kann. Norwegen hat kürzlich Pilotversuche mit einem Mixsystem durchgeführt."

Dubuis geht davon aus, dass dieses System – bei entsprechendem politischen Willen – in zwei bis drei Jahren auch in der Schweiz eingeführt werden könnte.

Pionierland

E-Voting ist eine relativ neue Technologie. Nur in wenigen Ländern weltweit werden verbindliche Versuche bei politischen Wahlen und Abstimmungen durchgeführt.

Auf dem europäischen Kontinent verfolgen neben der Schweiz Norwegen, Estland und neu Frankreich diesen Ansatz.

Die Sektion Politische Rechte der Bundeskanzlei und ihr Projektteam Vote électronique arbeiten in den internationalen Gremien mit und bringen die Erfahrungen der Schweiz in die Diskussionen ein. Sie nehmen an internationalen Konferenzen teil und pflegen den Austausch zu anderen Ländern, die Versuche durchführen oder planen.

Schönheitsfehler: Papier

Ein Nachteil, ein grober Schönheitsfehler bleibt: Trotz dem informatischen und elektronischen Aufwand "braucht es den Postkanal als Vertrauensanker", sagt Haenni. Die Codes müssen auf Papier beim Wähler ankommen, der elektronische Weg muss aus Sicherheitsgründen ausgeschlossen werden.

Wissenschaft und Forschung arbeiten seit Jahren an der dritten Generation des E-Votings, die auf einem Zusatzgerät basiert.

"Der Computer oder das Smartphone kann mir theoretisch immer etwas vormachen. Man kann diesen Geräten nicht 100 Prozent trauen. Dieses Problem kann man nicht grundsätzlich lösen", sagt Haenni.

Deshalb haben die Forscher des RISIS vor zwei Jahren im Auftrag der Bundeskanzlei ein Modell entwickelt, das auf einem rein elektronischen System basiert und den aufwändigen und teuren Postkanal ausschliesst.

Lösung: Zusatzgerät

Die Lösung besteht aus einem zusätzlichen Gerät, ähnlich den Geräten, die Banken für das E-Banking ihren Kunden verteilen, also einem Gerät "mit möglichst wenig Funktionen, das nicht an das Internet angeschlossen ist, also möglichst reduziert, nicht programmierbar und kostengünstig ist", sagt Haenni.

Diese Geräte fotografieren die Stimme, also den Wahl-Code auf dem Computerbildschirm und senden ihn anschliessend per USB-Kabel oder eine Funktechnologie an den Computer und von dort auf den Zentralrechner. Das Datenpaket bleibt im ganzen Prozess verschlüsselt. Zusätzlich ist der Geräte-Zugang zu ihnen durch einen PIN-Code geschützt.

Vertrauen wie in eine Banknote

"Das Vertrauen gegenüber einem solchen Gerät muss so gross sein wie das Vertrauen gegenüber einer Schweizer Banknote. Die Geräte müssten von der Bundeskanzlei zertifiziert sein", sagt Dubuis und räumt ein, dass "noch einige Fragezeichen" offen seien, "aber es ist kein Hirngespinst. Wir müssen noch einiges an Forschungsarbeit leisten und es ist auch eine Frage des politischen Willens. Man kann auch verschiedene Funktionen zusammenlegen".

Das heisst: Offen sind Fragen bei der Logistik der Verteilung, offen sind Fragen der Kosten, nicht nur für Produktion und Distribution, sondern auch für die Betreuung, denn PIN-Codes können vergessen gehen, ein Gerät, das man nicht regelmässig braucht, kann leicht unauffindbar werden oder Batterien können sich entladen.

Dubuis denkt auch an ein Gerät, das auch andere Behördenkontakte und gleichzeitig den Kontakt zur Bank elektronisch ermöglichen würde. Wieso denn nicht gleich das Gerät einsetzen, das fast jede und jeder immer auf sich trägt, das Smartphone?

"Die Hersteller der Smartphones könnten einen zweiten, nicht programmierbaren Betriebs-Modus einbauen. Das wäre technisch möglich", sagt Haenni. Der erste Modus wäre mit Apps und anderer Software, also auch mit Malware programmierbar. Der zweite, nicht programmierbare Betriebsmodus wäre sicher. Es könnte sich keine Malware einnisten.

Eine Idealvorstellung, die kaum realisierbar ist, denn "die Hersteller haben den Weltmarkt vor ihren Augen, da spielt die Schweiz keine Rolle", sagt Dubuis.

Andreas Keiser, swissinfo.ch
Biel

Links

- RISIS: E-Voting Group
- Schweizerisches E-Voting-Kompetenzzentrum
- E-Voting in der Schweiz und im Ausland
- Bundeskanzlei: E-Voting

URL dieses Artikels

- http://www.swissinfo.ch/ger/politik_schweiz/Papierloses,_sicheres_E-Voting_ein_Langzeit-Projekt.html?cid=37028496